# Отчёт Центра мониторинга ЗАО «ПМ» за третий квартал 2016 года

## Что и как мы считали

В рамках данного отчёта:

- **Событие ИБ** — идентифицированное появление определённого состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.
- **Инцидент ИБ** — появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.

Источниками событий выступают сетевые и хостовые IDS, сетевые устройства, сканеры защищённости, антивирусные решения и honeypot'ы.

В рамках внутренней обработки мы классифицируем инциденты в зависимости от затронутых ресурсов:

- **Инциденты высокой критичности**. Инциденты, связанные с ключевыми ресурсами серверного сегмента или с критичными ресурсами пользовательского сегмента (ресурсы, обрабатывающие критичную с точки зрения бизнеса, финансов или законодательства информацию).
- **Инциденты средней критичности**. Инциденты, связанные с некритичными ресурсами серверного сегмента.
- **Инциденты низкой критичности**. Инциденты, связанные с некритичными ресурсами пользовательского сегмента (рядовой пользователь).

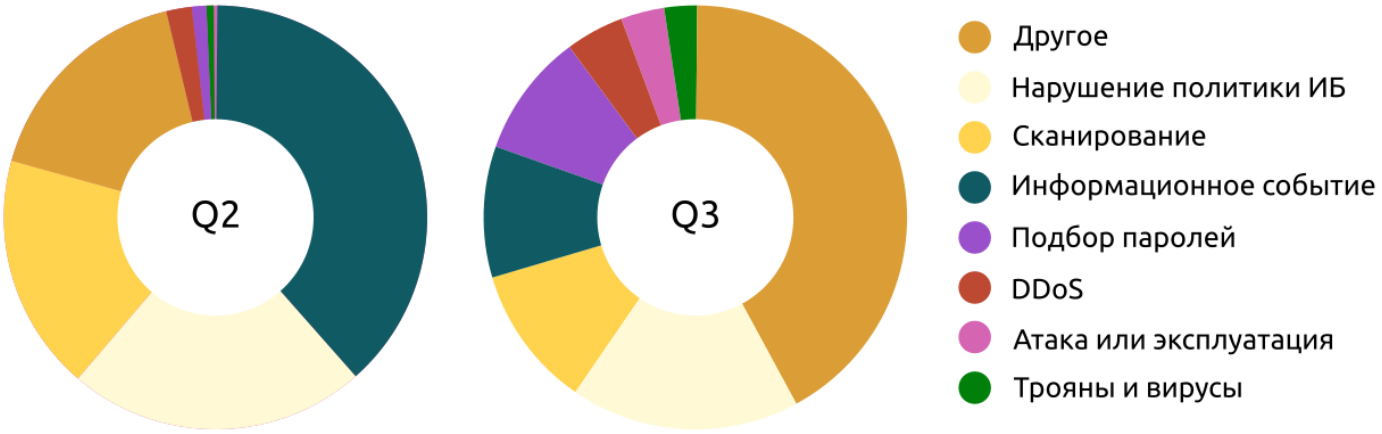
Аналитик Центра мониторинга может произвольно определить степень критичности, если посчитает, что инцидент может привести к серьёзным негативным последствиям.

## Результаты мониторинга

В период с 1 июля по 30 сентября сотрудники Центра мониторинга контролировали информационные системы нескольких организаций с общим числом подключённых узлов около 1 500 (рабочие места, веб, почта, файловые хранилища, VPN и т.д.).

За три месяца сенсоры зафиксировали и проанализировали **25 264 645 событий** информационной безопасности и выявили **21 инцидент**.

Классы проанализированных событий




«Информационное событие» (в предыдущем отчёте «Информация») — события, несущие информационную направленность, которые могут быть полезны при разборе инцидента.

«Нарушение политики ИБ» (в предыдущем отчёте «Политики ИБ») — события, свидетельствующие о действиях, предположительно нарушающих требования Политики ИБ контролируемой организации.

«Атака или эксплуатация» (в предыдущем отчёте «Атаки») — события, свидетельствующие о попытках удалённого исполнения кода или эксплуатации уязвимостей на контролируемых ресурсах.

«Сканирование» — события, свидетельствующие об исследовании сети перед попыткой атаки.

«Подбор паролей» — события, свидетельствующие о попытках получения доступа к контролируемым ресурсам путём подбора аутентификационных данных.

«Трояны и вирусы» — события, свидетельствующие о факте заражения контролируемых ресурсов вирусами или активности вредоносного ПО.

«DDoS» — события, свидетельствующие о попытках осуществления распределённых атак на отказ в обслуживании.

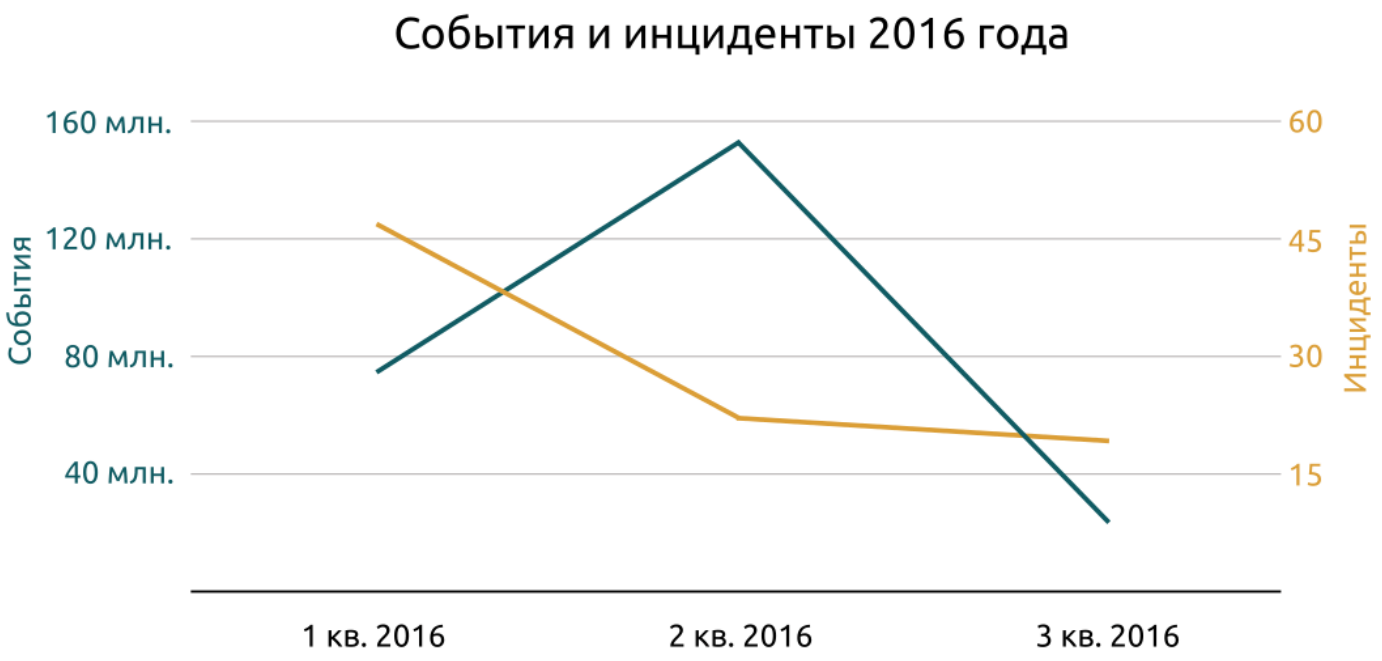
«Другое» — события которые по своей сути не могут быть отнесены к одному из вышеперечисленных классов.

Среди выявленного 21 инцидента:

| Класс инцидента | Высокая критичность | Средняя критичность | Низкая критичность | Всего инцидентов | Доля инцидентов |
|---|---|---|---|---|---|
| Вредоносное ПО | 2 | | 7 | 9 | 42,8% |
| DDoS | 2 | 1 | | 3 | 14,3% |
| Нарушение политики ИБ | 2 | | 1 | 3 | 14,3% |
| Подбор паролей | 5 | | | 5 | 23,8% |
| Атака | | | | 0 | 0,0% |
| Эксплуатация уязвимостей | | 1 | | 1 | 4,8% |
| Всего: | | | | 21 | 100,0% |


Наиболее актуальными и критичными из выявленных являются атаки, связанные с попытками получения несанкционированного доступа к ресурсам организаций.

За предыдущий второй квартал 2016 года Центр мониторинга зафиксировал **150 392 000 событий** ИБ и **23 инцидента**.

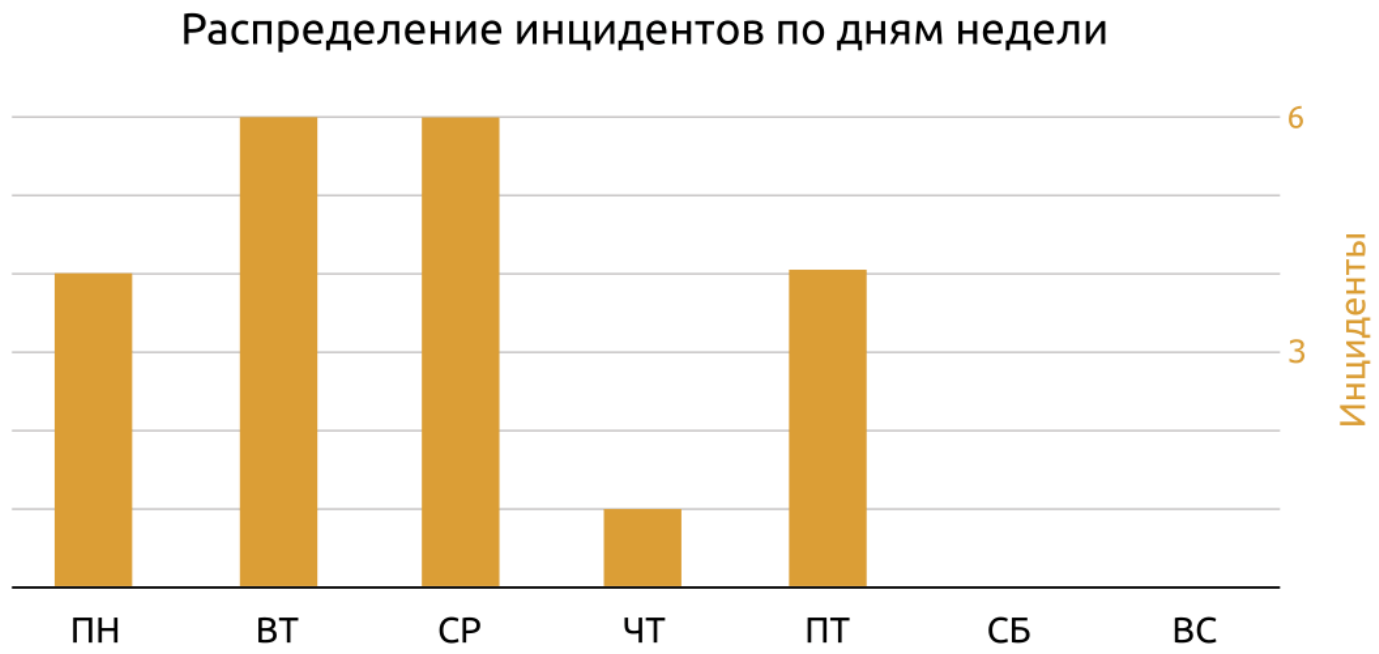



| | Доля инцидентов, % | | |
|---|---|---|---|
| Класс инцидента | 1 кв. 2016 | 2 кв. 2016 | 3 кв. 2016 |
| Вредоносное ПО | 84,6 | 43,5 | 42,8 |
| DDoS | | 8,7 | 14,3 |
| Нарушение политики ИБ | 2,6 | 30,4 | 14,3 |
| Подбор паролей | 5,1 | 17,4 | 23,8 |
| Атака | 7,7 | | |
| Эксплуатация уязвимостей | | | 4,8 |

Резкое снижение количества зарегистрированных событий ИБ обусловлено тремя факторами:

1. Сигнатурные аналитики доработали несколько десятков сигнатур, которые давали большое число false-positive срабатываний в конкретной контролируемой информационной системе.
2. Были оптимизированы некоторые правила базы AM Rules. Благодаря этому множество одинаковых событий теперь «склеиваются» в одно.
3. Благодаря первым двум пунктам Центр мониторинга быстрее реагирует на DDoS-атаки и помогает предотвращать их развитие на ранней стадии.

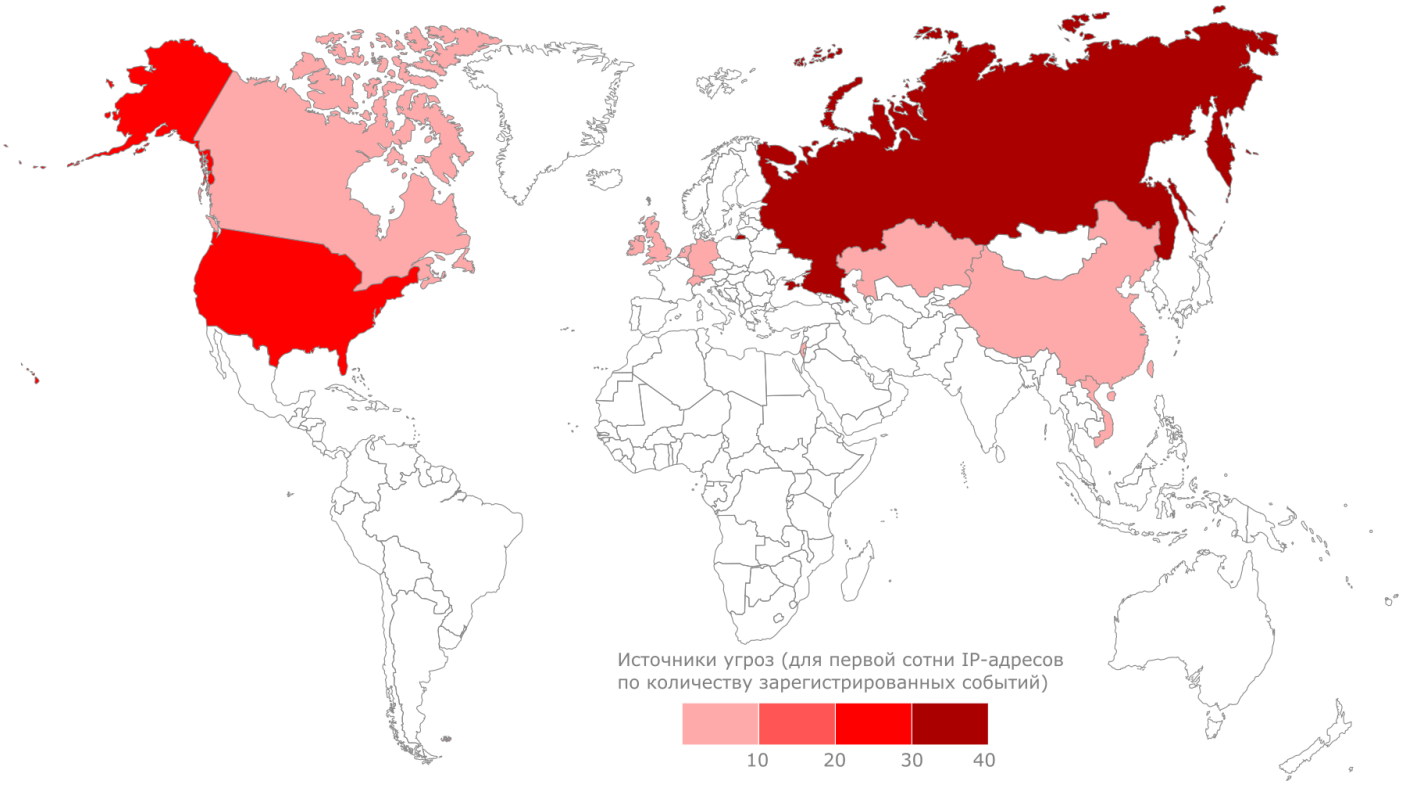
Распределение инцидентов ИБ относительно дней недели в третьем квартале 2016 года:




В этом квартале ситуация очень похожа на предыдущий период — пик инцидентов приходится на середину недели. Пользователи хотят расслабиться, заходят на развлекательные сайты с сомнительной безопасностью и получают вредоносное ПО. Серьёзных негативных последствий для контролируемых информационных систем такие инциденты не несут, но администраторы тратят время на антивирусные проверки, а пользователи в это время не могут полноценно работать.

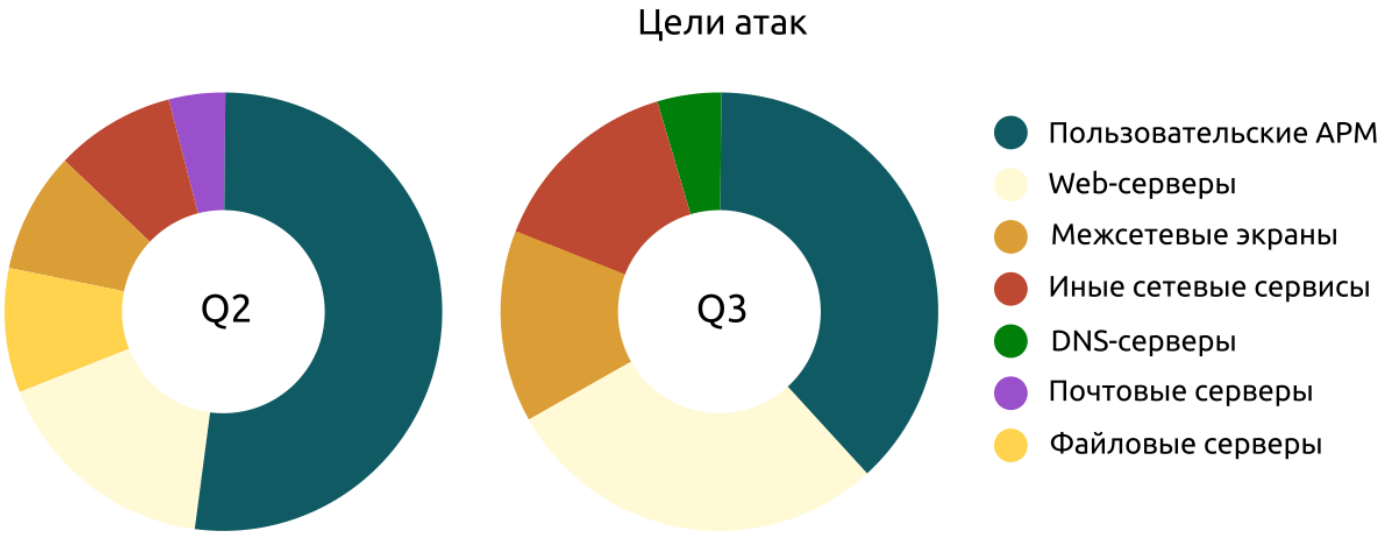
Распределение инцидентов ИБ за третий квартал 2016 года:

# ТОП источников




# ТОП подверженных инцидентам сегментов

Ситуация по целям атак изменилась непринципиально: наибольшую активность злоумышленники проявляли в отношении пользовательских рабочих мест и web-серверов, потому что это самые доступные для атак сегменты.



# Наиболее часто используемые техники воздействия на системы, повлекшие инцидент ИБ

| Угроза | Техника воздействия |
|---|---|
| Рекламное ПО | Заражение конечной системы, передача на командный сервер информации о пользователе, показ таргетированной рекламы. |
| Перебор паролей | Попытки подбора аутентификационной информации для доступа к сервисам и ресурсам контролируемых организаций — RDP, SSH, SMB, DB, Web. |
| Нарушение политик ИБ | Нарушение пользователями/администраторами контролируемых ресурсов требований политик ИБ в части использования устаревших версий или недоверенного ПО. Данное ПО может быть использовано злоумышленником для реализации атаки путём эксплуатации уязвимости. |
| Вирусное ПО (черви) | Заражение конечной системы, распространение вируса по локальной сети, отключение/блокировка служб, препятствующих распространению вируса, попытки проведения иных атак внутри сети для получения критичной информации и передачи на командные серверы. |
| DDoS с использованием ресурсов организации | DDoS Amplification — техника подмены своего адреса на адрес жертвы и генерации запросов небольшого размера к открытым сервисам. На запрос сервис возвращает ответ в несколько десятков раз большего объема на адрес «отправителя». Используя большое количество ресурсов различных организаций, злоумышленник осуществляет DDoS-атаку на жертву. |